Information Risk Management Policy

LLWR recognises that there are risks associated with the handling of information during the conduct of official business. The LLWR Board acknowledges that managing this information risk is an essential element in the framework of good Corporate Governance and is an integral part of good management practice. Effective Information Risk Management requires a balance to be struck between the cost of controlling information risks and the anticipated benefits that will be derived from effectively exploiting information. This Information Risk Management policy will set out LLWR's commitment and approach to Information Risk Management.

LLWR Commits to:	We will achieve this by:
Ensuring there is adequate governance arrangements in place to safeguard Confidentiality, Integrity and Availability.	Appointing a Senior Information Risk Owner (SIRO) at Board level to take overall responsibility for the Information Security Governance Framework Ensuring that the Information Security Governance Framework is supported by an Information Security Strategy and an Information Security Assurance Programme. Assigning Information Asset Owners (IAO) and compiling an Information Asset Register of all Information Assets.
Providing a coherent Information Risk Management Framework where information risks can be identified, considered, managed and shared.	Appointing a Chief Information Security Officer (CISO) to advise the SIRO on the risks to information. Setting an Information Risk Appetite and using an Information Risk Methodology that will allow for risk-based decisions to be made around information management. Using an information risk methodology that enables the analysis of risk to its business critical information, systems, processes and applications and within the supply chain.

Information Risk Management Policy

Protecting LLWR from information risks that would have a significant likelihood or impact on LLWR strategic goals and objectives.

Protecting information to a level proportionate to its value to the organisation.

Ensuring the equivalent level of protection is provided to LLWR information within the supply chain.

Employing good Cyber Hygiene practices to deter all but the most determined and skills threats.

Meeting Legal and Regulatory requirements including GDPR.

Ensuring that security is maintained in accordance with the Cyber Security and Information Assurance Policy.

Responding to Information Security events in order to remove attackers and prevent additional data compromise.

Having Incident Response, Business Continuity and Disaster Recovery Plans in place to recover Information and Cyber Systems to a safe and operationally viable state.

Having a positive information risk culture.

Ensuring that all personnel involved in managing information risks are trained to an appropriate level.